IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE: BPS DIRECT, LLC and CABELA'S, LLC, WIRETAPPING	MDL NO. 3074 2:23-md-03074-MAK

PLAINTIFFS' SUPPLEMENTAL
MEMORANDUM IN OPPOSITION TO MOTION TO DISMISS

MDL Plaintiffs, by and through undersigned counsel, hereby submit the following supplemental memorandum advising the Court of counsel's availability for a continued virtual oral argument on November 14 or 15, 2023, to the extent the Court believes it necessary or helpful and addressing the issues identified by the Court in its Order of October 26, 2023 (ECF No. 71).

MDL Plaintiffs' counsel is available at the Court's discretion on either November 14 or 15, 2023, for a continued virtual oral argument on the issues identified or any other topic for which the Court believes argument is necessary or helpful to resolution of Defendants' Motion to Dismiss (ECF No. 54-1). The questions for which supplemental arguments are requested are addressed in turn.

Question 1: Whether Website Users sufficiently alleged facts to establish Defendants accessed Website Users' computers without authority under 18 U.S.C. § 1030(a) with their best supporting authority.

Question 1. Plaintiffs pled specific facts alleging Defendants accessed Website Users' computers without their authority and obtained information from their protected computers in violation of 18 U.S.C. § 1030(a)(2)(C). Compl. ¶¶ 89, 92, 101-02, 107-08, 113-14, 120-21, 125-26, 130-31, 135-36, 145-48, 187-88. *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), is instructive. In *Drew,* a case involving a misdemeanor charge under § 1030(a)(2)(C) (the same section under which Plaintiffs proceed for civil liability), the court identified three required elements: 1) accessed without authorization or exceeded authorized access of a computer; 2) access involved interstate communication; and 3) by exceeding authorized access to a computer, defendant obtained information from a computer used in interstate communication. *Id.* at 457. The *Drew* court "noted that the latter two elements of the section 1030(a)(2)(C) crime"—that is, accessing a computer involved in interstate commerce and obtaining information by unauthorized access—"will always be met when an individual using a computer contacts or communicates with an Internet website." *Id.* The third element requires "obtaining information from a protected computer." *Id.* 18 U.S.C. § 1030(e)(2)(B) defines a protected computer as one "which is used in or affecting interstate or foreign commerce or communication[.]" *Id.* The court held "as a practical matter, a computer providing a web-based application accessible through the internet would satisfy the interstate communication requirement." *Id*. Importantly, the statute defines "exceeds authorized access" but does not define "intentionally," "accesses a computer" and "without authorization." *Drew* at 459. The court's thorough analysis explained the requisite intent is more than mistaken, inadvertent or careless, and involves abuse of a computer to obtain information. *Id*. at 459. The court defined "access" and "authorization" broadly according to their dictionary meanings to mean, respectively, "any interaction between two computers" and "to give approval or permission for." *Id.* at 459-60. Plaintiffs allege the statutory elements.

Question 2: As to the wiretap claims under the federal, California, and Missouri laws, Website Users provide support for their argument that party status and consent exceptions do not apply and clarify whether Defendants are parties to the communications at issue.

Question 2. The party and consent exemptions do not insulate Defendants from liability for Plaintiffs' wiretap claims. *First*, the party exemption fails because Defendants were not parties to all of the communications the SRPs intercepted. ¶¶ 1, 7, 90, 259, 268, 299, 312, 342, 405 (alleging instances of content captured without interaction, *e.g.*, IP address or location); *see also In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 806 F.3d 125, 142-43 (3d Cir. 2015) (parties to a conversation are the intended recipients); *Jurgens v. Build.com, Inc.*, 2017 WL 5277679, at *5 (E.D. Mo. Nov. 13, 2017) (plaintiff's intentional website submissions made defendant a party to those communications). And, even where Defendant was the intended recipient of Plaintiffs' communications, the exemption fails because Defendants secretly and contemporaneously allowed Plaintiffs' communications to be captured by SRPs. *In re Facebook Internet Tracking,* 956 F.3d 589, 607 (9th Cir. 2020) ("Permitting…unauthorized duplication and forwarding of unknowing users' information [would allow] the [party] exception to swallow the rule.") Moreover, SRPs were never parties to Plaintiffs' communications, creating liability under Cal. Pen. Code § 631. *See Valenzuela v. Nationwide Mut. Ins. Co.*, No. 2:22-cv-06177-MEMF-SK, 2023 WL 5266033, at *7 (C.D. Cal. Aug. 14, 2023) (finding website monitoring company was a third party and holding website owner liable under § 631). Thus, the party exemption does not apply here.

Second, the consent exemption fails because (1) Defendants cannot consent to the interception of communications where they were not a party, and Defendants' later *use* of these interceptions (*i.e.*, those without any party's consent) is a distinct violation of wiretap laws, 18 U.S.C. § 2511(d); (2) the scope of consent cannot be determined this early, *Doe v. Meta Platforms, Inc.,* 2023 WL 5837443, at *5 (N.D. Cal. Sept. 7, 2023); and (3) Plaintiffs never consented to the interceptions at issue, *see Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *7 (N.D. Cal. Aug 7, 2023) (consent requires explicit notice).

Question 3: As to the wiretap claims under the federal and Missouri laws, Website Users respond to Defendants' arguments and cited case law in support of their position Website Users fail to allege a criminal or tortious purpose (ECF No. 54-1 at 19-22, ECF No. 57 at 15-16).

Question 3. Defendants' argument against the application of 18 U.S.C. § 2511(2)(d) turns on whether Plaintiffs have adequately alleged that they engaged in the collection and interception of their communications with the intent to use it in a criminal or tortious manner. *See* ECF No. 54 at 20-21, ECF No. 57 at 15-16. As the court in *In re Google Inc.* noted, Plaintiffs need only plead "that the offender intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording." 806 F.3d 125, 145 (3d Cir. 2015). Here, Plaintiffs allege Defendants collected their personal information to aggregate it into detailed consumer profiles in order to individually target them with advertisements. Compl. ¶¶ 29, 31, 42, 45-46. Plaintiffs allege Defendants create "fingerprints" to uniquely identify Website Users and to track them across websites to monitor their consumer habits. *Id*. ¶¶ 45-47, 79-80. This allows Defendants to peer into Website Users' habits and interests as they travel to unrelated websites well after their information has been intercepted and is a separate violation of Plaintiffs' right to privacy. *See Planned Parenthood Fed'n of Am., Inc., v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016) (holding "defendants' subsequent disclosures of the contents of the intercepted conversations for the alleged purpose of further invading the privacy of plaintiffs' staff satisfies" the exception). Defendants employed tracking software to invade the privacy of Plaintiffs both at the time of collection and each subsequent time they visit a website that detects the "fingerprint" assigned to the Website User. *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067-68 (N.D. Cal. 2021) (association of plaintiff data with preexisting user profiles independently satisfies the criminal or tortious use exception). Thus, it is Defendants' (and its SRP's) subsequent aggregation and use of Plaintiffs' information that demonstrates Defendants' intent to invade the privacy of Plaintiffs even after their visit to the Website has ended. See *Democracy Partners v. Project Veritas Action Fund*, 285 F. Supp. 3d 109, 124 (D.D.C. 2018).

Question 4. As to the wiretap claims under the federal and Missouri laws, provide your best authority as to how we should consider applying the "criminal or tortious purpose" exception.

Question 4. While there is scant authority discussing the criminal or tortious exception to the Missouri Wiretap Act, because the Missouri statute contains near identical language as that of 18 U.S.C. § 2511(2)(d), authorities analyzing the Federal Wiretap Act are useful in determining the scope of the Missouri statute. *State v. Barrett*, 41 S.W.3d 561, 564 (Mo. Ct. App. 2001); *State v. King*, 873 S.W.2d 905, 908 (Mo. Ct. App. 1994). In analyzing the application of the criminal or tortious purpose exception of 18 U.S.C. § 2511(2)(d), several district courts have addressed the issue of when a criminal or tortious purpose is separate and distinct from the underlying wiretapping. For example, in *Democracy Partners v. Project Veritas Action Fund*, the Court noted that while trespass and fraudulent misrepresentation allowed for the interception, the criminal or tortious purpose of the wiretapping was to thereafter breach a fiduciary duty by disclosing the information so obtained. 285 F. Supp. 3d at 109. Similarly, and particularly relevant here, in *Brown v. Google LLC*, the court specifically noted that the alleged purpose of the wiretapping was to aggregate the collected information in order to build consumer profiles and direct subsequent targeted advertisements at those individuals. 525 F. Supp. 3d at 1067-68. *Planned Parenthood Fed'n of Am., Inc., v. Ctr. for Med. Progress* also analyzes the distinction between the underlying violation of the law by intercepting information, and the intent to subsequently use that information for a tortious purpose. 214 F. Supp. 3d at 828. Conversely, in the authority relied upon by Defendants, *In re DoubleClick Inc. Priv. Litig.*, the Court noted that "DoubleClick's cookies *only* collect information concerning users' activities *on DoubleClick-affiliated Web sites.* Thus, if a user visits an unaffiliated Web site, the DoubleClick cookie captures no information." 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001). The distinction in *DoubleClick* was that the information was not subsequently used to track Website Visitors, unlike what Plaintiffs allege here.

Question 5: As to the wiretap claims under the Maryland and Massachusetts laws, describe whether and to what extent our analysis differs given the definitions of "contents" under each State's law.

Question 5. First, Plaintiffs sufficiently allege that the HTTP request-response communications triggered by Plaintiffs' interactions with Defendants' website all contain sufficient information concerning the substance, purport and meaning of their communications. Compl. ¶¶ 65, 66 & n.5, 68, 206. Both the Maryland Wiretapping and Electronic Surveillance Act ("MWESA") and Massachusetts Wiretapping Statute ("MWS") broaden the definition of "contents" compared to their federal and state counterparts to include "any information *concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication.*" Md. Code Ann., Cts. & Jud. Proc. § 10-401(4); Mass. Ann. Laws ch. 272, § 99(B)(5). The addition of language pertaining to the identities of the parties, as well as the existence of the communications themselves, have urged courts to hold these definitions as notably "broad definition[s] of 'contents.'" *See Commonwealth v. Du*, 103 Mass. App. Ct. 469, 470 (2023) ("broad definition" of contents under MWS required suppression of surreptitious recordings made using software application on a telephone as the definition of contents "extends beyond the words of the communication itself or an aural recording of it"); *see also Alves v. BJ's Wholesale Club, Inc.*, 2023 WL 4456956, at *4 (Mass. Sup. Ct. June 21, 2023) ("keystrokes, clicks, mouse movements, URLs, and other data" are plausibly contents because "the Massachusetts statute defines 'contents also to include 'information concerning the identity of the parties' or 'the existence . . . of that communication'"). Broadly, Plaintiffs allege that the session replay creates a record of the "existence" of the communications by its very nature. Specifically, Plaintiffs allege that the SRC Defendants use identifies the communicating website visitors, including Plaintiffs. Compl. ¶¶ 76-78. As such, while Plaintiff's allegations meet the language of contents broadly, Plaintiffs also allege additional aspects of the communications which constitute "contents" under MWESA and MWS.

Question 6: As to the wiretap claims under the federal, California, and Maryland laws, provide your strongest authority as to whether Website Users allege a contemporaneous interception.

Question 6: The Complaint's detailed factual allegations more than sufficiently plead "contemporaneous interception" of Plaintiffs' communications for purposes of the Federal Wiretap Act, CIPA, and MWESA.[1] *See, e.g.*, Compl. ¶¶ 5-7, 64-87, 89-95, 138-45, 153, 178, 206, 267-69. Particularly where the method of interception is alleged, courts consistently conclude that the procurement of third-party software to record visitors to a website—like Defendant's use of SRC here—constitutes "contemporaneous interception." *See, e.g.*, *Luis v. Zang*, 833 F.3d 619, 627-34 (6th Cir. 2016); *Garcia v. Yeti Coolers, LLC*, 2023 WL 5736006, at *4 (C.D. Cal. Sept. 5, 2023); *Valenzuela v. Nationwide Mut. Ins. Co.*, 2023 WL 5266033, at *5 (C.D. Cal. Aug. 14, 2023); *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *3 (N.D. Cal. June 9, 2023).

The process by which SRC intercepts website visitors (*see, e.g.*, Compl. ¶ 5), and the process by which Defendants surreptitiously acquire Plaintiffs' communications "contemporaneously" with their transmission, raises factual questions that cannot be resolved on a motion to dismiss, as well-pled allegations as to SRC's "contemporaneous interception" are accepted as true. *See Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1048 (N.D. Cal. 2018) ("[W]here the precise nature of the software may be the determining factor in whether electronic communications were 'intercepted,' [the court] must accept plaintiffs' allegations as true and leave resolution of the issue on a developed record."); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 848 (N.D. Cal. 2014) (same); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014) (same).

[1] Neither the Federal, California, nor Maryland statute explicitly requires that the acquisition of a communication occur contemporaneously with the transmission of the communication. *See* 18 U.S.C. § 2510(4); Cal. Penal Code § 630 *et seq.*; Md. Code Ann., Cts. & Jud. Proc. § 10-401 *et seq*. Nonetheless, courts interpreting the statutory language have concluded that an "intercept" under each statute requires contemporaneity. *See, e.g.*, *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003). *See also Luis v. Zang*, 833 F.3d 619, 627-629 (reviewing cases and explaining the basis for the contemporaneity requirement) (6th Cir. 2016).

Question 7: As to the wiretap claims under the Maryland, Massachusetts, and Pennsylvania laws, provide your strongest authority as to whether session replay software is a "device."

Question 7. Software such as SRC is a device under MWESA, MWS, and WESCA. All three statutes broadly define "device" to imply that the class of technology contemplated by the statutes is extensive, and nothing in the plain language of the statutes indicates that a device is limited to a tangible object, as the Defendants contend. Indeed, applying the plain language of these three statutes, courts in each of these jurisdictions have recognized that software, such as SRC, can be a device under the relevant statutes or have otherwise recognized that whether software is a device is an issue of fact not to be addressed at the motion to dismiss stage. First, a Maryland court concluded that a software application installed on a smartphone used to record a conversation was a device under MWESA. *Holmes v. State*, 182 A.3d 341, 350–51 (Md. Ct. Spec. App. 2018). If a smartphone application is a device under the MWESA, so is SRC. Second, a Massachusetts court has expressly addressed whether SRC is a device under the MWS. *See Alves*, 2023 WL 4456956, at *5 (applying the plain language of Mass. Gen Laws. Ch. 272, § 99(B)(3) and concluding that SRC can be an "intercepting device" for the purposes of the MWS). This Court should follow *Alves* and reach the same conclusion. Third, Pennsylvania courts have indicated that whether software is a device under WESCA is a question of fact better addressed after discovery. *See Popa v. Harriet Carter, Gifts Inc*, 426 F. Supp. 3d 108, 117 (W.D. Pa. 2019); *Oliver v. Noom, Inc.*, 2:22-cv-01857-WSS (W.D. Pa. Aug. 22, 2023), ECF 28 at 13 (explaining that "[a]s alleged," Noom's SRC "could reasonably be considered a 'device or apparatus'" and that discovery would enable "the opportunity to develop a factual record" for website deployment of SRC and how SRC "interacted with each website user's browser and computer"). By contrast, no Pennsylvania court has held that SRC is *not* a device. The Court should follow caselaw from the applicable jurisdictions and conclude that SRC is a device, or, at worst, address the issue after fact discovery.

Question 8: As to the invasion of privacy claims, Website Users shall address the impact, if any, of *Kurowski v. Rush System for Health*, No. 22-5380, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023) and respond to Defendants' arguments (ECF No. 54-1 at 37, ECF No. 57 at 21).

Question 8. In *Kurowski*, the court dismissed invasion of privacy claims because third parties (not the defendant) intercepted private information and the plaintiff voluntarily gave it to defendant. *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 2349606, at *9 (N.D. Ill. Mar. 3, 2023). While the tort of invasion of privacy has four distinct theories, the two that are relevant—intrusion upon seclusion and public disclosure of private facts—are improperly conflated in *Kurowski*. *Id*. In short, the case was wrongly decided.

Here, Plaintiffs' claims are within the intrusion upon seclusion theory, which *Kurowski* correctly states does not require disclosure to a third party. *Id.* However, the converse is not true—just because there is disclosure does not mean there was not also an initial unlawful intrusion to obtain the facts disclosed. In *Feldman v. Star Trib. Media Co. LLC*, No. 22-CV-1731 (ECT/TNL), 2023 WL 2388381, at *4 (D. Minn. Mar. 7, 2023), an online newspaper shared the plaintiff's video history with Facebook, when plaintiff considered that history private. The court held that the defendant intentionally interfered with the plaintiff's seclusion by then sharing that information with Facebook. *Id*. The court reasoned that, under the Restatement of Torts, an interference with one's seclusion amounts to an invasion of privacy. *Id*.

According to *Kurowski*'s logic, no invasion of privacy occurs if someone "voluntarily" shares private information with another—regardless of whether the second party surreptitiously permits or procures a third-party eavesdropper. Taken further, this would permit *anyone* to invite third parties to intercept private communications, *i.e.*, a customer support line could let a stranger secretly listen in because the customer was voluntarily speaking on the phone. *Kurowski* wrongly confines privacy protection to information solely within the possession of the Plaintiff, denying that there is still a privacy interest in protecting a communication with a known party from disclosure to unknown third parties. This Court should not maintain such an artificial distinction.

Question 9: As to the claim under California Unfair Competition Law, Website Users shall address the impact, if any, of *Moore v. Centrelake Medical Group*, 83 Cal. App. 5th 515 (Cal. App. Ct. 2022) on their standing arguments and respond to Defendants' arguments (ECF No. 54-1 at 44-45, ECF No. 57 at 23).

Question 9. *Moore v. Centrelake Medical Group*, 83 Cal. App. 5th 515 (Cal. App. Ct. 2022) has no bearing on Plaintiffs' standing under the UCL, and Defendant's reliance on it is misplaced. In *Moore*, the court was addressing an appeal of a demurrer and found that the lower court was wrong in dismissing the UCL claim for lack of standing. The court found that the plaintiff had standing based on several theories. *Id.* at 527-32. The diminution of value theory was not necessary for the court's decision because it reversed based on other theories. The language that Defendant relies on here was in dicta, in a section called "Guidance on Remand," where the appellate court was directing the lower court regarding what to do on remand and was expressing its opinion on the diminution of value theory. *Id.* at 538-42. Instead of following such dicta,[2] this Court should follow the reasoning in *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) which relies in part on a Ninth Circuit decision,[3] and find that Plaintiffs' allegations here regarding diminution of value of their PII are sufficient to plead lost money or property under the UCL for purposes of a 12(b)(6) motion.

Defendant's argument that Plaintiffs do not allege they ever attempted or intended to participate in a market for their information, or otherwise to derive economic value from their data is of no moment, because that is not required. *See, e.g. Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1190-91 (D. Nev. Nov. 2, 2022) (collecting cases and noting that "these pleading requirements, that Plaintiffs must establish both the existence of a market for their PII and an impairment of their ability to participate in that market, is not supported by Ninth Circuit precedent and other district courts in this Circuit have rejected them."). Accordingly, Defendant's motion to dismiss Plaintiffs' UCL claim should be denied.

---

[2] The other District Court decisions Defendants rely on merely reflect other judges' non-binding views.

[3] *In re Facebook Privacy Litigation*, 572 F. App'x 494, 494 (9th Cir. 2014).

Question 10: As to Plaintiff Tucker's claim under the Missouri Merchandising Practices Act, Website Users shall provide support for their argument the Act is not limited to consumers who make purchases in the marketplace.

Question 10. The word "purchase" is not statutorily defined in § 407.025. As a result, Plaintiffs contend that "unfair practice" is broadly defined to include unlawful and deceptive practices that occur when a consumer is attempting to purchase a consumer product for the reasons stated in the Opposition. According to the Supreme Court of Missouri, "[t]he literal words ['unfair practice'] cover every practice imaginable and every unfairness to whatever degree." *Ports Petroleum Co. Inc. of Ohio v. Nixon*, 37 S.W.3d 237, 240 (Mo. 2001) (*en banc*). Nevertheless, Plaintiff seeks leave for Plaintiff Arlie Tucker to amend his complaint allegations to allege the purchase of a product in his dealings with Defendants.

Date: November 2, 2023

By: */s/ Nicholas A. Colella*

Nicholas A. Colella (PA Bar # 332699)
Gary F. Lynch (PA Bar # 56887)
Kelly K. Iverson (PA Bar # 307175)
Jamisen Etzel (PA Bar # 311514)
Elizabeth Pollock-Avery (PA Bar # 314841)
Patrick Donathen (PA Bar # 330416)
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
NickC@lcllp.com
Gary@lcllp.com
Kelly@lcllp.com
Jamisen@lcllp.com
Elizabeth@lcllp.com
Patrick@lcllp.com

Kate M. Baxter-Kauf
Karen Hanson Riebel
Maureen Kane Berg
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

Katrina Carroll
LYNCH CARPENTER, LLP
111 W. Washington St. Suite 1240
Chicago IL 60602
Tel: (312) 750-1265
katrina@lcllp.com

Joseph H. Kanee
MARCUS & ZELMAN LLC
701 Brickell Avenue, Suite 1550
Miami, FL 33131
Tel: (786) 369-1122
joseph@marcuszelman.com

Ari H. Marcus (PA Bar # 322283)
MARCUS & ZELMAN LLC
701 Cookman Avenue, Suite 300

Asbury Park, NJ 07712
Tel: (732) 695-3282
ari@marcuszelman.com

Plaintiffs' Co-Lead and Liaison Counsel

Carey Alexander
SCOTT & SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue
Ste 17th Floor
New York, NY 10169
Tel: (212) 223-6444
calexander@scott-scott.com

MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Tel: (404) 978-6971
mgibson@thefinleyfirm.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street Fourteenth Floor
New York, NY 10004
Tel: (646) 357-1100
snathan@hausfeld.com

James J. Pizzirusso (Md. Bar No. 20817)
HAUSFELD LLP
888 16th Street N.W. Suite 300 Washington, D.C. 20006
(202) 540-7200
jpizzirusso@hausfeld.com

Plaintiffs' Steering Committee